MULTIMEDIA UNIVERSITY®

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2022/2023

ECE3256 CYBERSECURITY

(All Sections / Groups)

3 JULY 2023
9:00 A.M – 11:00 A.M.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 12 printed pages including the cover page with 4 questions only.

2. Attempt all FOUR (4) questions. All questions carry equal marks and the distribution of marks is given in the questions.

3. Please print all your answers in the answer booklet provided.

4. State all assumptions clearly.

Question 1

(a) You unexpectedly received an urgent email from a bank as shown in Figure Q1(a).

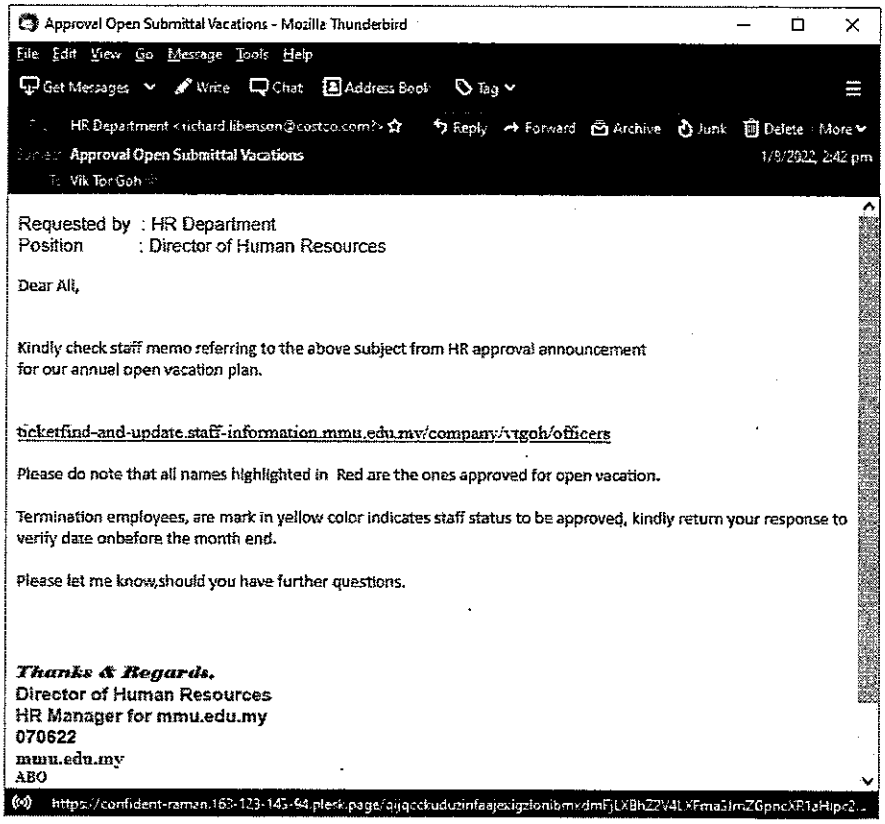

Approval Open Submittal Vacations - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages Write Chat Address Book Tag
HR Department <richard.libensen@costco.com> Reply Forward Archive Junk Delete More
Approval Open Submittal Vacations
1/9/2022, 2:42 pm
To: Vik Tor Goh
Requested by : HR Department
Position : Director of Human Resources
Dear All,
Kindly check staff memo referring to the above subject from HR approval announcement for our annual open vacation plan.
ticketfind-and-update.staff-information.mmu.edu.my/company/vtgoh/officers
Please do note that all names highlighted in Red are the ones approved for open vacation.
Termination employees, are mark in yellow color indicates staff status to be approved, kindly return your response to verify date onbefore the month end.
Please let me know,should you have further questions.
Thanks & Regards.
Director of Human Resources
HR Manager for mmu.edu.my
070622
mmu.edu.my
ABO

Figure Q1(a)

(i) Is the email legitimate or otherwise?

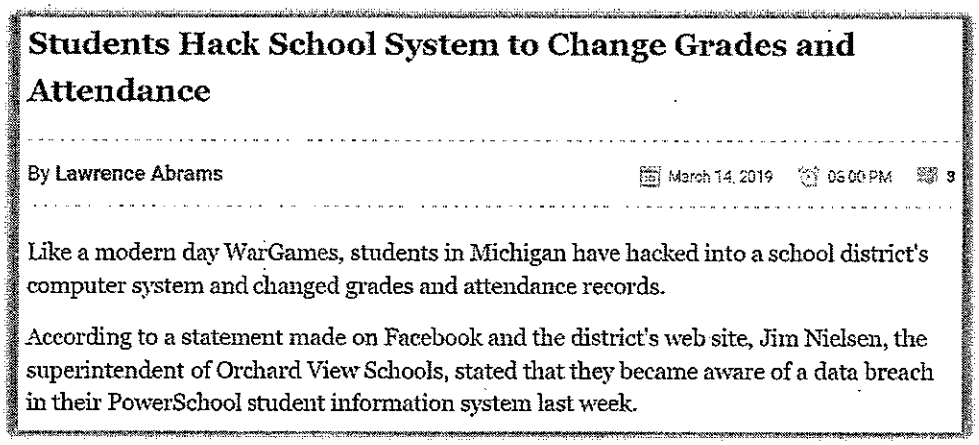
[1 mark]

(ii) Justify your answer in Part (a)(i) by describing at least **THREE (3)** signs or indicators that may indicate whether the email is legitimate or otherwise.

[6 marks]

(b) The news snippet shown in Figure Q1(b) describes a cybersecurity incident that had occurred.

Continued...



Students Hack School System to Change Grades and Attendance

By Lawrence Abrams March 14, 2019 06:00 PM 3

Like a modern day WarGames, students in Michigan have hacked into a school district's computer system and changed grades and attendance records.

According to a statement made on Facebook and the district's web site, Jim Nielsen, the superintendent of Orchard View Schools, stated that they became aware of a data breach in their PowerSchool student information system last week.

Figure Q1(b)

(i) Which **ONE (1)** of the three cybersecurity goals best describes this incident. Justify your answer in the context of the news snippet.

[2 marks]

(ii) Describe the goal that you answered in Part (b)(i).

[2 marks]

(iii) Explain **ONE (1)** control method that could have been applied to prevent this incident from happening in the first place.

[2 marks]

(c) Scams are criminal activities that often result in victims losing their reputation, money, and even health. The news article in Figure Q1(c) reports such a scam.

(i) Name and describe this type of attack.

[2 marks]

(ii) There are four psychological traits that a scammer can use in this type of attack. List down the psychological trait(s) that the scammer in the news article used.

[2 marks]

(iii) For each of the psychological trait that you listed earlier in Part (c)(ii), elaborate on how that trait was exploited in relation to the news article shown in Figure Q1(c).

[4 marks]

Continued...

Senior citizen conned of over RM650,000 in Macau Scam

JOHOR BARU: A 68-year-old retiree here has lost his hard-earned savings of RM652,500 to fraudsters in a Macau Scam.

Johor Commercial Crime Investigation Department (CCID) chief Asst Comm Amran Md Jusin said the caller impersonated a policeman and used scare tactics during a telephone call, accusing the senior citizen of consuming prohibited substances and money laundering.

"The suspect told the victim that his bank account would be audited and investigated because of his alleged activities.

"The retiree was then instructed to transfer the money from his bank account into a personal bank account number provided by the caller to aid in the so-called investigation.

"The suspect also claimed that a court order had been issued and told the victim to cooperate," he said in a statement on Monday (June 20).

The victim then transferred RM652,500 into the provided bank account via 22 transactions from May 11 to June 5, said ACP Amran.

Figure Q1(c)

(d) You had been tasked with designing your organisation's security infrastructure.

(i) What is the name of the multi-layered approach that you can consider implementing?

[1 mark]

(ii) Briefly describe this approach and its advantage.

[1 mark]

(iii) Give **TWO (2)** examples of the tools, controls, or mechanisms that can be implemented to achieve this multi-layered approach.

[2 marks]

Continued...

Question 2

(a) The company that you work for has developed their own proprietary cryptosystem. However, your manager has decided that the cryptographic algorithm cannot be audited by third parties for fear that the strength of the cryptosystem will be compromised.

As a security professional, what are your opinions on this matter? Do you agree or disagree with your manager? Justify your arguments.

[Note: Although there is a generally accepted answer, you can answer differently. You will be evaluated on your justification, reasoning, and critical thinking.]

[2 marks]

(b) The Vigenère Cipher is a type of polyalphabetic cipher and the Vigenere Table is shown in Figure Q2(b).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure Q2(b)

(i) Encrypt the message "mastery" using the keyword "break".

[2 marks]

(ii) Decrypt the ciphertext "MNYEGD" with the keyword "magic".

[2 marks]

Continued...

(iii) What is the keyword if the ciphertext is "UMEMJQQR" for the message "decision".

[2 marks]

(c) Using AES, perform the following operations.

(i) Express the following plaintext as an AES state.

Plaintext: {6B C2 BE E2 2E 40 7F 96 E9 3D 5E 11 73 93 17 3A}

[1 mark]

(ii) Using the AES state from Part (c)(i), what is the output of **AddRoundKey** if the key is given as "00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F".

[2 marks]

(iii) Assume that the AES state in Part (c)(i) is the input into the **SubBytes** function. What is the output state after SubBytes using the S-Box in Figure Q2(c).

[3 marks]

(iv) Subsequently, show the output state after the **ShiftRows** function is applied on the results of Part (c)(iii).

[3 marks]

hex	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

x

The Substitution Table – Sbox[xy] (in hexadecimal)

Figure Q2(c)

Continued...

(d) Consider the RSA cryptosystem with $p = 5$, $q = 19$ and $e = 7$.

(i) Calculate n and t.

[2 marks]

(ii) Find the corresponding decryption key, d using the given parameters.

[2 marks]

(iii) Write down the formulas for encryption and decryption.

[2 marks]

(iv) Subsequently, encrypt the message, $m = 8$ using the appropriate formula from Part (d)(iii).

[2 marks]

Continued...

Question 3

(a) Access to your company's website has been unstable and intermittent. You examine the server's configurations, and everything is in order. You check the firewall, server logs, and router logs but do not find any penetration or hacking attempts, except for very high network usage. You then check the web server's access log files and notice an excessively large amount of data requests from the same set of IP addresses. This raises your suspicions that your company is experiencing an attack.

(i) What is the most likely attack based on your analysis?

[1 mark]

(ii) What are the goals or objectives of this attack?

[2 marks]

(iii) Is this a type of active or passive attack? Justify your answer.

[2 marks]

(iv) How can you mitigate this type of activity?

[2 marks]

(b) Describe the following types of network attacks and **ONE (1)** of their corresponding mitigation methods:

(i) Network sniffing.

[3 marks]

(ii) OS identification.

[3 marks]

(iii) Man-in-the-middle.

[3 marks]

(c) As the new Security Officer in your organisation, you plan on implementing link encryption for all remote workers who wish to access the company's network.

(i) What are the benefits of link encryption?

[2 marks]

(ii) Which is more secure, end-to-end encryption or link encryption? Justify your answer.

[2 marks]

Continued...

(iii) A Virtual Private Network (VPN) is a type of link encryption. Explain the tunnel mode of operation for a VPN.

[2 marks]

(iv) Name at least **ONE (1)** popular Virtual Private Network (VPN) service that is often advertised in YouTube videos.

[1 mark]

(v) Besides privacy and confidentiality, these popular VPN services also allow a user to stream videos from another region. For example, Netflix users in Malaysia can watch USA-only videos. How does a VPN achieve this?

[2 marks]

Continued...

Question 4

(a) Briefly describe the following terms:

(i) Program vulnerability.

[2 marks]

(ii) Software bug.

[2 marks]

(iii) Exploit.

[2 marks]

(iv) Software patch.

[2 marks]

(b) Study the C code shown in Figure Q4(b).

```
#include <stdio.h>

int main ()
{
    int score = 82;
    char name[20];

    printf("Enter name: ");
    gets(name);

    return 0;
}
```

Figure Q4(b)

(i) Is it susceptible to buffer overflow?

[1 mark]

(ii) Justify your answer in Part (b)(i).

[2 marks]

(iii) How can a buffer overflow vulnerability be prevented?

[2 marks]

Continued...

(c) As a security analyst working in a security operations centre, you routinely examine server log files for suspicious activities. A sampling of an Apache webserver log file is shown in Figure Q4(c) on the last page of this question paper.

(i) Is there an attack on the webserver?

[1 mark]

(ii) Name the type of attack if present, otherwise answer "None".

[2 marks]

(iii) Justify your answer in Part (c)(ii), even if there is no attack.

[3 marks]

(iv) The webserver log file shows **network activity on the server**. What is the name of the attack if the **network traffic is spied on without permission when it moves through the network**?

[1 mark]

(v) How can you prevent the attack that you named in Part (c)(iv)?

[2 marks]

(d) BB Clinic has a computer used to store patient records such as name, treatment, and prescription. The records are updated daily when a patient visits. They require daily backups but have limited storage space.

(i) What is the most suitable backup method?

[1 mark]

(ii) Justify your choice in Part (d)(i).

[2 marks]

Continued...

```
41.214.40.213  [07/02/2016:07:22:16] GET /wordpress/process.php?search=joered&dept=finance
134.15.64.203  [07/02/2016:07:22:19] POST /wordpress/wp-login.php?uname=admin&passwd=s3rv3r@LPkd
41.214.40.213  [07/02/2016:07:22:23] GET /wp-content/uploads/2015/02/1620528.jpg
178.255.215.65 [07/02/2016:07:32:07] GET / wp-content/comments/feed/
84.55.41.57    [07/02/2016:07:33:16] POST /wordpress/wp-login.php?uname=admin&passwd=je#56vGSegef
84.55.41.57    [07/02/2016:07:33:17] POST /wordpress/wp-login.php?uname=admin&passwd=je#56vGSegeg
178.255.215.65 [07/02/2016:07:38:19] GET /wp-content/js/customscript.js
178.255.215.65 [07/02/2016:07:39:25] GET /wp-content/images/arrow.png
84.55.41.57    [07/02/2016:07:40:16] POST /wordpress/wp-login.php?uname=admin&passwd=je#56vGSegeh
178.255.215.65 [07/02/2016:07:42:25] POST /wp-admin/admin-ajax.php?id=345323&vs=exec
178.255.215.65 [07/02/2016:07:42:34] GET /wp-admin/admin.php?cf_action=sync_comments&post_id=307
178.255.215.65 [07/02/2016:07:42:04] GET /wp-content/great/style.css
178.255.215.65 [07/02/2016:07:42:05] GET /wp-content/plugins/twitter-feed.css?ver=4
84.55.41.57    [07/02/2016:07:42:16] POST /wordpress/wp-login.php?uname=admin&passwd=je#56vGSegei
41.214.40.213  [07/02/2016:07:43:05] GET /wp-includes/js/jquery/jquery-migrate.min.js
41.214.40.213  [07/02/2016:07:43:05] GET /wp-content/disqus/disqus.js?ver=3
41.214.40.213  [07/02/2016:07:43:05] GET /wp-content/images/arrow.png
84.55.41.57    [07/02/2016:07:44:16] POST /wordpress/wp-login.php?uname=admin&passwd=je#56vGSegej
41.214.40.213  [07/02/2016:07:44:19] GET /wp-content/images/search.png
178.255.215.65 [07/02/2016:07:45:19] GET /index.php?option=com_phocagallery&view=category&id=1
```

Figure Q4(c)

End